CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

*Екип за реагиране при инциденти в компютърната сигурност*

# Мониторинг на актуалните киберновини – към 08.12.2020 г.


## Съдържание

## Фокус върху националните възможности за киберсигурност: Нова рамка за самооценка, която да даде възможности на държавите-членки на ЕС

Агенцията на ЕС за киберсигурност издава Национална рамка за оценка на способностите (NCAF), за да помогне на държавите-членки на ЕС да измерват нивото на зрялост на своите национални възможности за киберсигурност.

07 декември 2020 г.

Защо рамка за оценка на способността?

Възможностите за киберсигурност са основните инструменти, използвани от държавите-членки на ЕС за постигане на целите на техните национални стратегии за киберсигурност. Целта на рамката е да помогне на държавите-членки да изградят и подобрят способностите за киберсигурност чрез оценка на тяхното ниво на зрялост.

Рамката ще позволи на държавите-членки на ЕС:

- Извършване на оценка на техните национални възможности за киберсигурност.
- Увеличаване зрелостта на информираността;
- Определяне областите за подобрение;
- Изграждане на нови възможности за киберсигурност.

Можете да изтеглите доклада на ENISA - Национална рамка за оценка на възможностите

**Произходът на концепцията**

Разработена с подкрепата на 19 държави-членки на ЕС, тази рамка е проектирана след обширен обмен на идеи и добри практики. Стратегическите цели на националните стратегии за киберсигурност служат като основа на проучването.

Рамката е разработена като част от мандата на ENISA, както е определено в Закона за киберсигурност. Той попада под разпоредбата за подкрепа на държавите-членки на ЕС в изграждането на капацитет в областта на националните стратегии за киберсигурност чрез обмен на добри практики.

**Основните характеристики**

Рамката за самооценка се състои от 17 цели, структурирани около 4 клъстера. Всеки от тези клъстери е свързан с ключова тематична област за изграждане на капацитет за киберсигурност. С всеки клъстер са свързани различни цели. Въз основа на 5 нива на зрялост бяха измислени конкретни въпроси за всяка цел.

Клъстерите са както следва:

(I) Управление и стандарти за киберсигурност - Това измерение разглежда аспекти на планирането за подготовка на държавата-членка срещу кибератаки, както и стандарти за защита на държавите-членки и цифровата идентичност

(II) Изграждане на капацитет и осведоменост - Този клъстер оценява способността на държавите-членки да повишават осведомеността относно рисковете и заплахите за киберсигурността и за това как да се справят с тях. Освен това този клъстер измерва способността на страната непрекъснато да изгражда способности за киберсигурност, да увеличава знанията и уменията в областта на киберсигурността.

(III) Правни и регулаторни - Този клъстер измерва капацитета на държавите-членки да въведат необходимите правни и регулаторни инструменти за справяне с киберпрестъпността и също така да се справят със законови изисквания като докладване на инциденти, въпроси, свързани с поверителността, CIIP.

(IV) Сътрудничество - Този клъстер оценява сътрудничеството и обмена на информация между различни групи от заинтересовани страни на национално и международно ниво.

**За повече информация:**

https://www.enisa.europa.eu/news/enisa-news/national-cybersecurity-capabilities-framework

## Как DMARC може да спре престъпниците да изпращат фалшиви имейли от името на вашия домейн

7 декември 2020 г.

Технологиите на 21-ви век позволяват на киберпрестъпниците да използват сложни и неоткриваеми методи за злонамерени дейности.

През 2020 г. проучване разкрива, че 65% от базираните в САЩ компании са уязвими към фишинг атаки  и атаки с имитация на имейли. Това изисква надграждане на сигурността на вашата организация с DMARC, което, ако не бъде приложено, ще позволи на кибер-нападателите да:

- Поискват парични преводи от уязвими служители чрез фалшиви имейли, като се представят за старши ръководители в компанията
- Изпращат фалшиви фактури до вашите служители и партньори
- Правят сделки с незаконни стоки чрез вашия домейн
- Разпространяват Ransomware
- Се представят за поддръжка на клиенти, за да откраднете поверителна информация за клиент или партньор

Подобни ситуации могат да имат дълготрайни последици за вашия бизнес. От нанасяне на удар върху репутацията и доверието на марката сред нейните партньори и клиентска база до загуба на ценна фирмена информация и милиони евро, рисковете са безброй.

**Какво е подправяне на домейн?**

Подправянето на домейни е много често срещана форма на нарушаване на сигурността, при което киберпрестъпник се опитва да използва домейн на бизнес имейл на фирма, за да извърши редица злонамерени дейности, като подправи адреса на подателя.

Нападателите създават надеждни полета в имейлите, които изпращат, за да увеличат шансовете те да изглеждат легитимни и по този начин да бъдат отворени от получателите. Целта на подправянето на домейни е да подмами потребителите да повярват, че имейлът идва от удостоверен източник и да ги манипулира да взаимодействат с измамния имейл, в който са вградени злонамерени връзки, сякаш е легитимен.

Чудите се как атакуващите управляват това? Това се улеснява от липсата на протокол за удостоверяване на имейл в организацията. Имейл домейните обикновено работят чрез SMTP (Simple Mail Transfer Protocol), което представлява комуникационен протокол, който позволява прехвърлянето на поща чрез цифрови платформи. Той обаче има свои собствени ограничения като например липсата на автоматизиран механизъм за удостоверяване на имейл, програмиран в него. Киберпрестъпниците се възползват от тази уязвимост, за да фалшифицират имейл домейни и да изпращат измамни имейли, представяйки се за вас.

Подправянето на имейли може да има тежки последици и да доведе до загуба на поверителна информация за компанията или да предизвика парични преводи от партньори или служители, докато някой се представя за висш ръководител на компанията. Можем да разберем по-добре пейзажа на заплахата, като разгледаме няколко реални примера:

През октомври 2020 г. Бюрото за преброяване на населението на САЩ предупреди срещу хакери, които се опитват да фалшифицират домейни, като ги използват за стартиране на фишинг измами и кражби на удостоверения. Те дадоха информация за 63 новорегистрирани домейни, представящи се за Бюрото за преброяване на населението в САЩ.

Базирана в Ню Йорк търговска фирма в средата на август заяви, че е загубила 6,9 милиона долара в измама с Business Email Compromise (BEC) през май 2020 г. и повече от 80% от компаниите в САЩ твърдят, че са били засегнати от Business Email Compromise след пандемията.

Настъпването на Черния петък и Кибер понеделник през месец ноември 2020 г. допълнително увеличи шансовете за фалшифициране на домейни на популярни магазини на дребно под маската на атрактивни оферти и карти за подарък, изпратени до тяхната клиентска база от нападатели.

**Как DMARC може да защити вашия бизнес?**

DMARC, или Домейн-базирани съобщения за удостоверяване на автентичност и съответствие, е протокол за удостоверяване на имейл, създаден с цел да осигури бизнес домейни и марки от фалшифициращи атаки. DMARC налага използването на комбинация от SPF и DKIM технологии за удостоверяване на имейли, за да гарантира, че до крайните потребители се доставят само реални имейли.

Без DMARC всички имейли, изпратени от имейл домейна на вашия бизнес, достигат до входящата поща на получателя без никаква проверка или без проверка на сигурността. При DMARC обаче агентът за прехвърляне на поща (MTA) на получателя търси SPF, DKIM и DMARC записите на името на домейна, за да удостовери изпращача. След като подателят бъде проверен или удостоверен, пощата попада във входящата поща на получателя.

Чрез удостоверяване на всички имейли, изпратени от вашия домейн, вие не само предотвратявате самозванците да злоупотребяват с името на домейна ви, за да извършват злонамерени дейности и пране на пари, но също така се подобрява

доставката на имейли, което кара вашите клиенти и партньори да реагират по-бързо на вашите имейли.

Внедряването на протоколи за удостоверяване на имейл във вашата организация ви помага да бъдете в течение на променящите се тактики на нападателите, да защитавате базите данни на вашата компания и да предотвратите финансови или информационни загуби.

**Защо да изберем PowerDMARC?**

За да бъдете в течение на непрекъснато променящите се тактики на киберпрестъпниците, изборът на механизми за наблюдение на DMARC и навременното докладване е също толкова наложително, колкото простото избиране на налагането на DMARC, за да се осигури видимост и подобряване на доставката на имейли. Ето защо трябва да се доверите на инструмент като PowerDMARC.

PowerDMARC не само включва механизми за удостоверяване на имейл с DMARC, но предоставя мащабируем набор от допълнителни функции, които далеч надхвърлят обичайните съоръжения:

**Автоматизирано удостоверяване на имейл**

- Многофункционалният инструмент за анализ DMARC на PowerDMARC улеснява процеса на преминаване към налагане на DMARC от p = none към p = отхвърляне / карантина за нула време! Той обезсилва страха от нарушаване на имейл системата, като прави процеса на изпълнение бърз и лесен, като осигурява пълна видимост и анализ, за да помогне на системните администратори да оптимизират своите изпращащи източници SPF / DKIM, за да се съобразят с политиката на DMARC.
- PowerBIMI осигурява хоствана BIMI Record услуга чрез присвояване на логото на фирмата си до имейл адреса, така че може лесно да се определят границите между фалшив и реални имейли. 3 лесни стъпки - качете вашето лого, генерирайте автоматизираните BIMI DNS записи и ги публикувайте в DNS на вашия домейн.
- Внедряването на PowerDMARC ви помага да получавате ежедневни отчети за имейлите, които преминават и се провалят при проверките за сигурност и DMARC проверката, с DNS сигнали в случай на пропуснати конфигурации в SPF, DMARC, DKIM и BIMI, заедно със forensic сигнали в реално време.

- Денонощните съоръжения за мониторинг от експерти по сигурността следят всички тези източници и откриват неупълномощени изпращачи, които се опитват да се представят за някой друг, със система за предупреждение в реално време за докладване на фалшиви атаки и преглед на историята на злоупотребата с домейни.
- Инструментът за мониторинг в реално време DMARC предлага пълна видимост на вашия имейл домейн, като наблюдава атаки за подправяне на имейли, които се извършват по целия свят чрез картографиране на заплахи.

**Forensic криптиране**

PowerDMARC ви дава възможност да получите подробна видимост на вашите отчети за откази на DMARC RUF (Forensics), заедно с неговия механизъм за разузнаване на заплахи и AI. Той също така ви позволява да криптирате хедърите за обратна връзка и хедърите на пощата на вашите DMARC Forensic RUF отчети, използвайки вашите собствени PGP ключове, за да осигурите абсолютна поверителност.

**PowerSPF**

Всеки път, когато вашият SPF запис използва механизми за определяне на получаващи сървъри как да обработват имейл, това води до DNS търсене. За предотвратяване на DoS атаки броят на DNS търсенията на SPF запис е ограничен до максимум 10. Следователно за организации, разчитащи на множество доставчици на трети страни, преминаването на ограничението за търсене на 10 DNS е неизбежно.

Веднага щом това се случи, дори одобрените входящи имейли ще се провалят при проверка на SPF! PowerSPF ви позволява да добавяте или премахвате податели във вашия SPF запис с лекота, така че винаги да оставате под ограничението за търсене от 10 DNS. Той решава проблема с "permerror", грешките при запис на SPF, ограниченията и проблемите с конфигурацията на една платформа.

**Програма MSSP**

PowerDMARC е платформа на MSSP DMARC SaaS с множество клиенти, която предлага на MSP / MSSP / партньорите възможността да препродават услугата с пълен контрол за управление и осигуряване на собствени клиенти.

Чрез партньорството си с PowerDMARC можете да получите достъп до табло за управление на множество клиенти, заедно със специални цени, опции за първокласна поддръжка и независими средства за оптимизация.

**За повече информация:**

https://thehackernews.com/2020/12/how-dmarc-can-stop-criminals-sending.html